Review: "Control, Trust, Privacy, and Security: Evaluating Location-Based Services"

The Navtrak Website proudly tells businesses that "with the Navtrak GPS vehicle tracker, your [fleet] insurance risks decrease dramatically…."In October 2003, Wired reported that "The Georgia Institute of Technology is sponsoring a study using global positioning systems to track the movements of cars and monitor the motoring habits of their drivers."

A common complaint among those who like to imagine vast government conspiracies and alien abductions is that of the feared "implant," essentially a radio frequency ID (RFID) chip, used to track the recipient's movements.

The following is the fourth and last review of articles about ethical and philosophical considerations for security and privacy in technology from the Spring 2007 (vol. 26, #1) issue of IEEE Technology and Society Magazine.

"*Control, Trust, Privacy, and Security: Evaluating Location-Based Services*" by Laura Perusco and Katina Michael

The use of location based services (LBS) has long been a figure in popular science fiction. Practical tracking of individuals for the benefit of society is not a new possibility, as the Wired quote indicates. Only recently has technology, cost, and desire merged to create the necessary atmosphere. Today, such an ability is even bragged about as a way for a business to save money.

Ms. Perusco and Ms. Michael use LBS in their article as a concrete example of technology's ethical ambiguity. Generally, an LBS is any service that uses the position of something for a specific purpose. GPS and RFID are examples of LBS.

The use of LBS creates special ethical and legal questions. Who has accountability for the accuracy and availability of location information? Under what circumstances can a user opt-in or -out of LBS? What are the rights of caregivers and guardians to the location information of their charges? How long is location information stored?

The authors use five short stories, which they call scenarios, to set up the discussion of these issues. Because the authors are from the University of Wollongong in Australia, they conduct their analyses from an Australian social and legal perspective.

There exists a serious disparity between technological progress and its implications for the future, especially in terms of security and privacy. This, the authors argue, requires increased scrutiny. Their article is one attempt.

The first scenario, "Control Unwired," explores vulnerability. Kate, working late in the big city, comes close to mortal peril as she struggles to use her PDA to locate and call a cab.

The second scenario, “The Husband and His Wife,” highlights the threat to personal autonomy. Unhappy Colin wears an RFID chip in his shirts so his wife Helen can keep track of his movements. She worries about his health after a scare with angina.

Next, “The Friends and Colleagues” examines group control. Scott and his girlfriend Janet debate the government’s increased use of RFID chips implanted into parolees. As a parole officer, Scott argues the benefits to society. Janet, though, worries that the government could expand tracking further into the general population.

The fourth and fifth scenarios combine to show the dangers of misplaced trust in technology. At a routine visit to a parolee, Scott checks that Doug’s RFID is functioning properly. After Scott leaves, we see that Doug has spoofed the system. He can leave the chip at home while he goes out for his own particular kind of fun.

Together, these scenarios present a bleak picture of people who have lost control over their autonomy. For example, we see Kate who cannot get a cab without the aid of her PDA, putting her safety in jeopardy. Then there’s poor Colin, whose movements are monitored and restricted by his well-meaning wife.

Additionally, we have examples of false security from LBS. Colin gets the better of his wife when the battery dies while she’s on a plane. Doug can go on the prowl after he cuts out his RFID.

In the real world, the situation is no better. The authors report that following the July 2005 London subway bombings, the Australian government passed laws allowing people merely suspected of terrorist activities to be tracked with wearable devices.

The scenarios prompt many questions, none of which have obvious answers. When can mere suspicion justify the ultimate invasion of privacy–our bodies? Who decides when intensive monitoring is for “our own good?”

A long running debate centers on whether technology is neutral or has an inherent social impact. “Guns don’t kill people; people kill people.”

Ms. Perusco and Ms. Michael state that “[t]hese situations [the stories] imply that LBS is not neutral, and that the technology is designed to enhance control in various forms.” (p. 11) In this case, though, they fail to mention that LBS are primarily used to monitor and control inventory, which most would consider neutral.

Technological determinism is the theory that technical developments drive the way we live. The authors counter that technologies which cannot find a market never develop enough to change society. For example, electronic tracking requires LBS. The use of LBS on people requires a society strongly concerned with security. Social needs and technology mesh.

Society must also be wary of the consequences of relying heavily on any technology. “If we become as reliant on LBS as we have become on other technologies like electricity, motor vehicles, and computers, we must be prepared for the consequences when (not if) the technology fails” (p. 12), write the authors.

As in the previous three articles from IEEE Technology and Society Magazine summarized here, “[t]he principal question is: how much privacy are we willing to trade in order to increase security?” (p. 13)

The authors ask whether the widespread use of LBS will have a long-term positive or negative on society and individuals? “[N]ot all secondary effects can be foreseen. However, this does not mean that deliberating on the possible consequences is without some genuine worth.”

Read all the articles in this series:

- “Review: Privacy and Security as Ideology“
- “Review: Designing Ethical Phishing Experiments“
- “Review: Good Neighbors Can Make Good Fences“
- “Review: Privacy and Security a Synthesis“

06.18.2007. | Categories: Literature Review